REMARKS/ARGUMENTS

The amendments and remarks hereto attend to all outstanding issues in the pending final Office Action of 16 May 2006. Claims 1-16 remain pending in this application (hereinafter, the "'402 Application), with claims 1, 2, 4-8 and 14-16 amended for clarity. Subtitled sections presented herein below correspond with the order of issues presented in the aforementioned Office Action.

Response to Arguments

The Examiner indicates that Applicant's arguments of February 28, 2006 (hereinafter, the "Prior Response") have been fully considered, but are not persuasive. We respectfully disagree. The prosecution history of the '402 Application, when reviewed, indicates fundamental differences in the way that the Examiner and Applicant interpret the Ulyanov patent. We believe that these differences are due primarily to the fact that quantum computing is a new, highly technical field, with relatively opaque terminology and semantics. Once several subtle but important terminology differences are exposed, we believe that the novelty of the application's claims will be evident. We therefore respectfully request the Examiner's careful consideration of both the following discussion and of the point-by-point reply to the Examiner's comments, provided thereafter.

Discussion

The Ulyanov Patent concerns "A methodology and an algorithm for programming a quantum logic algorithm". Ulyanov col. 43, lines 66-67. The '402 Application provides for "encrypting a program for execution on a remote host computer on a network, such that incorrect execution by the remote host computer is detectable, and such that the underlying software code remains secure, and such that the computations and the data associated with execution are unintelligible standing alone and otherwise useless at the host computer." Specification p. 1, final paragraph – p. 2, line 2. In particular, the claims of the '402 Application (as filed) are directed to a method for encrypting programs for encrypted execution on a network having a remote host computer, and a secured network for executing encrypted computer programs at a remote host computer without sharing intelligible or otherwise useful program code, computations or data associated with execution.

These objectives of the Ulyanov Patent and the present application are fundamentally different. Moreover, although the methods used by the Ulyanov Patent and the present application share some common terminology and superficially similar constructs, they are in fact decidedly different.

For example, Ulyanov teaches the implementation of a quantum algorithm based on a function expressed as an input-output "map" table. See Ulyanov col. 13, line 61- col. 14, line 6. Such a map table lists all possible inputs together with their corresponding outputs. This table explicitly defines a function in the Ulyanov patent and the Ulyanov patent teaches how to represent the desired input-output relationship as a unitary operator. By contrast, the present application describes a method for expressing a program as a unitary matrix. The difference between a map table representation and a program is fundamental and intrinsic.

Consider a "program" that sorts two binary integers into ascending order. The program, in pseudo-code, is for example:

```
read x;
read y;
if (x >y) then z:=x; x:=y; y:=z end;
write x;
write y;
```

The map table representation of the relation implemented by this program would enumerate all possible input and output pairs that this program would compute. For example, the following table:

Input X	Input Y	Output X	Output Y
10001	01101	01101	10001
10010	01101	01101	10010
00010	00001	00001	00010
00001	00010	00001	00010
...	...	...	...

would have 1024 lines to describe the relation defined by the above program for 5 bit inputs. If the inputs were 10 bit numbers, there would be over one million lines in the map table while the program description remains unchanged.

Ulyanov teaches the encoding of a map table or a function into a unitary matrix representation, while the present application teaches the encoding of a program as a unitary matrix. This is a fundamental difference between Ulyanov and the present application. Moreover, Ulyanov uses the term "encoding" in the sense of converting (as information) from one system of communication into another, for example, converting one representation (a map table or function) into another representation (a unitary matrix) just as a binary integer is an encoding of a base-10 integer or DNA is an encoding of genetic information.

On the other hand, Applicant's claims recite a method and a secured network for "encrypting" programs where, for example, if it is intercepted by a third party (e.g., Applicant's host computer) it cannot be read; only the persons/systems sending and receiving the information have the key and this makes it unreadable to anyone except the intended persons. See, Specification p. 8, lines 3-6. In other words, an objective of the present application is the remote execution of an encrypted program in its encrypted form. Accordingly, host computers are connected by a network (such as the Internet or LAN). For example, "Data for input to the program is...encrypted at control computer 12 or elsewhere 18 in the network 14 and sent to host 16 over network 14. Host 16 then executes an encrypted form of the program using the encrypted form of the data; and transmits results through network 14. Control computer 12 (or another computer with the decode information) then accesses and

decodes the results to determine the desired output." Specification p. 6, second paragraph.

The present application is concerned with "encryption" for example in the sense of hiding the meaning of a message from any party not authorized to access that meaning. The message is the program being executed and the data on which it executes. The meaning of this program and this data are hidden from the executing computer. Ulyanov does not involve any such "encryption" it only involves the aforementioned concept of "encoding".

Furthermore, Ulyanov does not teach a network, e.g., a computer network as recited throughout the '402 Application and now specified in the amended claims. The only networks mentioned by Ulyanov are a quantum network and a fuzzy neural network, both of which are different from Applicant's network, which can be "the Internet, a virtual private network, LAN or other network, wired or wireless, ***connecting computing devices together***." Specification p. 6, lines 1-2, emphasis added. For example, a quantum network is recognized as a model of quantum computation, and not an actual computer network.

Likewise, a fuzzy neural network is not an actual computer network, but a neural network based on fuzzy logic. In a neural network, simple nodes or neurodes connect together to form a network (neural network). The practical use of neural networks is realized with algorithms designed to alter the strength (weights) of the connections in the network to produce a desired signal flow. This accords with Ulyanov's weights. See, e.g., Ulyanov claims 5, 6, FIG. 1A and col. 5, lines 13-25. The nodes or neurodes of a fuzzy neural network are similar to individual circuits, gates or transistors of a circuit that are interconnected and communicate through wires (e.g., synapses), and not through the specified protocol by which networked computers communicate (e.g., TCPIP, HTTP, FTP).

To summarize this discussion, a map table and a program are fundamentally different representations, the former being the subject of the Ulyanov patent and the latter being the subject of the present application. Moreover, Ulyanov is concerned with "encoding" map tables as unitary matrices while the present application is concerned with "encrypting" programs as products of unitary matrices sampled from Haar distributions. Ulyanov makes no reference to Haar distributions or other types

of random distributions over unitary matrices, because Ulyanov is not concerned with encryption of programs, instead focusing on effective execution of certain types of quantum algorithms. The techniques and the goals for "encoding" in Ulyanov and "encrypting" in the present application are fundamentally different. Also, Ulyanov does not teach a network as recited and described in the '402 Application.

Point-by-point reply

(A) The Examiner disagrees with Applicant's argument that Ulyanov does not disclose encoding a program as a unitary matrix, stating "The program is encoded into unitary matrix Uf. The examiner asserts that a matrix is going to contain n rows and n columns." Final Office Action p. 2, "Response to Arguments," third paragraph.

Respectfully, the Examiner appears to miss Applicant's point. The Prior Response did not focus primarily on the substance of Ulyanov's matrix, but pointed out that Ulyanov discloses encoding a function into a unitary matrix operator U_F. This is different from encoding a program, as in Applicant's claims.

As is known in the art, and as noted in the above Discussion, a function is not the same as a program. A function is essentially a compact description of the relationship of one field, relative to the other. See, e.g., Ulyanov col. 16, lines 1-10. A function may for example be calculated using a program, but it is quite different from a program, which is commonly recognized as a set or sequence of instructions to be performed by a computer.

Respectfully, Ulyanov col. 13, line 61 – col. 14, line 6 (cited to support the Examiner's position) recites that "The ***function f is firstly encoded*** into a unitary matrix operator U_F that depends on the properties of f." Ulyanov col. 13, lines 64-66. We reiterate that this passage in Ulyanov summarizes a well known paper by David Deutsch, which does not discuss encoding a program as a unitary matrix with n rows and n columns, as a step in encrypting a program for encrypted execution. See Prior Response pages 4-5, discussion of *element (a)* for further detail.

(B) The Examiner next disagrees with Applicant's argument that Ulyanov fails to teach encoding an input data string to a general program as a vector of length n, in the context of encryption, as is required in claims 1 and 15. In particular, the Examiner asserts that "the vector will have a length" and that "The reference reads

upon having a vector of length n." Final Office Action p. 2, "Response to Arguments," fifth paragraph.

Again, respectfully, it appears that there is a misunderstanding of Applicant's prior arguments. Applicant did not dispute the length of Ulyanov's vector so much as point out that Ulyanov encodes a function into another function, which is then encoded into a UF map table. See Ulyanov, col. 15, lines 56-57. This is different from encoding an input data string to a program, especially when taken as a part of Applicant's encryption method. Furthermore, we note that the passage cited in support of the Examiner's position (in the Office Action of 11/29/05) describes development of a quantum gate. Ulyanov specifies that: "The term "gates" is not meant to imply that quantum computation can be physically realized in a manner similar to classical logic networks." Ulyanov col. 8, lines 63-65. On the other hand, Applicant's encrypted programs may be communicated over a standard LAN, a virtual private network or the Internet (Specification, p. 6, line 3) and executed on classical computers employing classic logic such as Boolean logic, for example.

(C) The Examiner next presents disagreement with Applicant's arguments that Ulyanov does not teach loading an encoded program and an encoded data string (with/on) a host computer. Respectfully, as noted above, Ulyanov teaches encoding functions, and not encrypting programs or data strings, as in Applicant's claims. Because Ulyanov does not recite or otherwise provide an encrypted program or an encrypted data string (that is encrypted to the program), it follows that Ulyanov can not (and does not) load such an encrypted program or data string encoded thereto.

In the Office Action of 11/29/05, the Examiner states that Ulyanov col. 16, lines 1– col. 17, line 67 teaches loading an encoded program/data string. Respectfully, this section again discusses functions, in the context of the Deutsch-Joza algorithm. It does not discuss loading an encoded program/data string on a host computer.

(D) The Examiner next disagrees with Applicant's position that Ulyanov does not teach executing an encoded program, using an encoded data string, on the host computer. Respectfully, once more, the Ulyanov section is cited in an attempt to show this element of Applicant's claims does not discuss program execution. Rather, the section discusses development of a quantum gate. Furthermore, once again,

Ulyanov encodes a function, and does not encrypt a program. Since Ulyanov does not provide an encrypted program, it follows that Ulyanov also can not and does not execute an encrypted program.

(E) Next, the Examiner disagrees with Applicant's argument that Ulyanov does not teach communicating results (in particular, results of executing the encoded program) from a host computer to a network. Once more, Ulyanov does not encode a program or execute an encoded program. Rather, Ulyanov encodes functions. Therefore, Ulyanov can not communicate results of executing an encoded program from a host computer to a network.

(F) Finally, the Examiner disagrees with Applicant's stance that Ulyanov does not teach decoding results into output representative of executing the program with the data string, wherein computations and data associated with the program and data string are unintelligible and useless at the host computer. The Examiner indicates that Figure 8 of Ulyanov shows decoding an encoded program. The Examiner states that "once the encoded program has been forwarded from the host computer, the results become useless to this device" and are "only discernible to the received device." Final Office Action p. 2, "Response to Arguments," fifth paragraph.

Again, we must respectfully disagree. Figure 8 does not show computations and data being useless at a host computer. The description of Figure 8 is completely silent as to such a feature. Rather, Figure 8 is an outline showing the structure of a quantum algorithm. See Ulyanov col. 13, lines 49-50. Again, Ulyanov nowhere teaches or even suggests such encryption.

Claim Rejections - 35 U.S.C. § 102

Turning now to the rejection of claims 1-16 under 35 U.S.C. § 102(e), we must again disagree with the Examiner. Given the above discussion and point-by-point reply, we believe that claims 1-16 are shown to be allowable "as is". However, in an attempt to eliminate the confusion apparently caused by the terminology used in the '402 Application and Ulyanov, claims 1-8 and 14-16 are amended to replace appearances of encoded/encoding programs and data strings with encrypted/encrypting programs and data strings, and to specify a computer network.

These amendments are fully supported by the '402 Application. For example, the '402 Application recites the following (emphasis added):

"In one aspect, the invention provides a method for encrypting a program for execution ***on a remote host computer on a network***, such that incorrect execution by the remote host computer is detectable, and such that the underlying software code remains secure, and such that the computations and the data associated with execution are unintelligible standing alone and otherwise useless at the host computer." Specification p. 1, final paragraph– p. 2, line 2..

"In another aspect, the method has the further step of ***embedding constants into the data and program prior to the step of encryption***," Specification p. 5, second paragraph.

"In operation, ***a program to be executed on host 16 is first encrypted on control computer 12 and sent to host 16 over network 14***. Data for input to the program is also encrypted at control computer 12 or elsewhere 18 in the network 14 and sent to host 16 over network 14. Host 16 then executes an encrypted form of the program using the encrypted form of the data; and transmits results through network 14. Control computer 12 (or another computer with the decode information) then accesses and decodes the results to determine the desired output." Specification p. 6, second paragraph.

"These operations occur through matrix multiplication. As described herein, this means that ***the program is first converted to a matrix of the form $A=(a_{ij})$, and that the input data for the program is converted to a vector of the form $b=(b_j)$***, such that A and b are compatible for multiplication...***A and b are next encrypted***". Specification p. 6, third paragraph.

"The important feature of encryption as described is that host computer 16 does not glean intelligible or otherwise useful information ***of the underlying program or program software code, or of the data and computations entered as input or generated thereby***." Specification p. 8, final four lines of first paragraph.

"Processing in a method 50 in accordance with the invention, as depicted in FIG. 2, begins at control computer 12 (or other computer in

network with host computer 16), identified as step 52...***step 56 converts a data string, for input to the program, to a vector b.***" Specification p. 8, second paragraph. See Specification p. 6, third paragraph, quoted above, for encryption of vector b.

As noted above, Ulyanov does not encrypt programs or data strings. Rather, Ulyanov recites encoding and decoding with respect to functions or map tables. For at least this reason, Ulyanov cannot anticipate claim 1 or claim 15, both reciting encrypted/encrypting programs and data strings. Claims 2-14 and 16 depend from claims 1 and 15, respectively, and benefit from like argument.

Further patentable differences in claims 1-16 include the following features, argued in further detail in our Prior Response.

Independent Claims 1 and 15:

In order to anticipate claims 1 and 15, Ulyanov must teach every element of the claim and "the ***identical invention*** must be shown in as complete detail as contained in the ... claim." *MPEP 2131*, citing *Verdegaal Bros. V. Union Oil Co. of California*, 814 F.2d 628, 2 USPQ2d 1051 (Fed. Cir. 1987) and *Richardson v. Suzuki Motor Co.*, 868 F2.d 1226, 9 USPQ2d 1913 (Fed. Cir. 1989), emphasis added.

We have shown that Ulyanov does not meet the requirements for anticipation, for example failing to teach encrypting a program or a data string. However, Ulyanov fails to teach other elements of Applicant's independent claims. For example, if Ulyanov does not teach encrypting a program or a data string, Ulyanov cannot teach the particulars of:

- encrypting a program as a unitary matrix;
- encrypting an input data string to the encrypted program...;
- loading an encrypted program and an encrypted data string (with/on) a host computer;
- executing an encrypted program using an encrypted data string (with/on) the host computer; and
- communicating results of executing the encrypted program using the encrypted data string.

In addition, as noted in the above discussion and point-by-point reply, Ulyanov does not teach or suggest computations and data associated with a program

and data string being unintelligible and useless at the host computer. Figure 8, cited by the Examiner in rejecting this claim element, outlines the structure of an algorithm. There is no suggestion, either in Figure 8 or in the description thereof, to indicate computations and data (of any type) being useless at a host computer; indeed, Ulyanov nowhere teaches or even suggests such encryption.

Furthermore, as also noted in the above discussion and point-by-point reply, Ulyanov does not teach encrypted execution on a computer network, as is also recited in independent claims 1 and 15. Anticipation is not established, because Ulyanov does not teach every element of the claims. Withdrawal of the Examiner's rejection of claims 1 and 15 is respectfully requested.

Dependent Claims 2–14:

Claims 2–14 depend from claim 1, either directly or through intervening claims. Claims 2–14 are therefore also not anticipated by Ulyanov, for at least the reasons laid out herein above. However, we submit that these claims are further allowable over Ulyanov, for additional reasons exemplified herein below.

Claims 2 and 3: The Examiner applies Ulyanov col. 16, line 1– col. 17, line 67; and col. 19, line 1 – col. 20, line 44 in an attempt to show anticipation of claims 2 and 3, respectively. However, these passages again summarize the aforementioned "Quantum Theory, the Church-Turing principle and the universal quantum computer," and do not teach conversion of a program to a unitary matrix multiplication (as required in claims 2 and 3), in the context of claim 1. We thus respectfully request withdrawal of the rejection of claims 2 and 3.

Claim 4: As amended, claim 4 recites that encrypting the program includes generating two independent identically distributed unitary matrices X, Y from the uniform probability distribution over U_n determined by the Haar distribution. Again, we must respectfully disagree with the Examiner's stance that Ulyanov teaches such generation. The passage cited by the Examiner describes the standard encoding of functions into unitary matrix multiplications. There is no discussion there or elsewhere in Ulyanov of generating independent, identically distributed unitary matrices from the Haar distribution. Ulyanov does not mention the Haar distribution. Absent such teaching (and because of the non-anticipated base claim), Ulyanov cannot anticipate claim 4.

Claim 5: Amended claim 5 requires computing U' as XUY* and communicating U' to a remote host computer over the network. Respectfully, contrary to the Examiner's statement, Ulyanov does not teach or discuss computing any product of the form XUY* where X and Y are randomly generated unitary matrices from the Haar distribution, nor does Ulyanov teach communicating any results with another computer. Withdrawal of the Examiner's rejection is respectfully requested.

Claims 6 and 7: Ulyanov does not teach the limitations of amended claim 6 or amended claim 7, in the context of claim 1. For example, Ulyanov does not teach computation of b' as Yb, and communicating b' to the remote host over the network, in the context of program encryption and encrypted execution. As noted, the Ulyanov passage cited by the Examiner (Ulyanov col. 16, line 1 – col. 17, line 67) recites standard encoding of functions into unitary matrix multiplications. It does not recite computing an input vector b' as a matrix vector product, Yb. We therefore respectfully request withdrawal of the rejection of claims 6 and 7.

Claims 8 and 9: These claims require:

- executing encrypted data strings including the steps of (a) computing the product of XUY* and Yb and (b) communicating results to the network (amended claim 8), and
- decoding the results into output, including computing X*XUb, external of the host computer, to determine the multiplication of Ub as desired output of the program, wherein XUY* and Yb is (XUb) and X*XUb is obtained by matrix multiplication X*(XUb) (claim 9).

Respectfully, Ulyanov does not teach or even mention elements (a), (b) of claim 8, nor does Ulyanov teach decoding the results into output as recited in claim 9. The col. 16, line 1 – col. 17, line 64 passage cited by the Examiner does not discuss or suggest computing the product of encrypted XUY* with encrypted Yb, or communicating such results over any network. Furthermore, Ulyanov col. 26, lines 6-42 describes the measurement properties associated with extracting results from a quantum computation. There is no mention there or elsewhere in the patent of decoding at the host computer encrypted results that were computed on a remote

computer. Withdrawal of the Examiner's rejections of claims 8 and 9 is thus respectfully requested.

Claim 10: Ulyanov col. 26, lines 6-42 is again cited, the Examiner now stating that the passage discloses "decoding comprising decrypting at a control computer connected to a network and a host computer," as in claim 10. However, this passage mentions neither a host computer, nor a control computer, nor a network. Further, there is no mention anywhere within Ulyanov of decrypting. In particular, Ulyanov does not even suggest decoding or decrypting results "into output representative of executing the program with the data string", where "computations and data associated with the program and data string are unintelligible and useless at the host computer" (limitations inherited from claim 1). Ulyanov therefore cannot anticipate claim 10, thus, we respectfully request withdrawal of the Examiner's rejection.

Claims 11-13: We must again disagree with the Examiner's assertions that Ulyanov "suggests" a network comprising the Internet, a virtual private network or a LAN. We searched the Ulyanov patent for the terms "Internet", "web", "virtual", "private", "LAN" and "local area network", and found all terms conspicuously absent from the reference. Furthermore, even if Ulyanov did "suggest" these limitations, such a suggestion would be insufficient to alone render an anticipation rejection. Pursuant MPEP §706.02(V):

> "for anticipation under 35 U.S.C. §102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be **inherently present**." (emphasis added)

Since the limitations of claims 11-13 are not directly taught, we believe that the Examiner is making an inherency rejection; however, regarding inherency, MPEP §2112 states:

> "In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic **necessarily** flows from the teachings of the applied prior art. *Ex parte Levy*, 17 USPQ2D 1461, 1464 (Bd. Pat. App. & Inter. 1990)."

The Examiner has not provided any factual or technical reasoning to support an inherently present Internet, virtual private or LAN network, as required per MPEP §2112, thus, inherency is not established and there is no anticipation of "suggested" features of claims 11–13. Withdrawal of the rejection of claims 11-13 is respectfully requested.

Claim 14: Amended claim 14 requires embedding one or more constants into an input data string or program, prior to encrypting, to detect incorrect execution or data tampering. For example, "This can be accomplished by appending a trailing 1, as $\begin{bmatrix} b \\ 1 \end{bmatrix}$, to the input data vector b and embedding U into an (n+1) by (n+1) unitary as $\begin{bmatrix} U & 0 \\ 0 & 1 \end{bmatrix}$ so that the correct output is $\begin{bmatrix} Ub \\ 1 \end{bmatrix}$. Any change to $X\begin{bmatrix} Ub \\ 1 \end{bmatrix}$ either through error or malicious tampering will result in a decoded answer that will not have exactly 1 as the trailing entry of the decoded output vector $\begin{bmatrix} Ub \\ 1 \end{bmatrix}$." Specification, p. 5, ¶2, lines 3–7.

Ulyanov does not teach such embedding. Rather, Ulyanov recites embedding an operator U_F "into a quantum gate G, where G is a unitary matrix." As shown throughout Ulyanov, U_F is not a constant. Rather, U_F "depends on the properties of f... In some sense, the unitary operator U_F calculates f when its input and output strings are encoded into canonical basis vectors of a complex Hilbert Space. U_F maps the vector code of every string into the vector code of its image by f. A squared matrix U_F on the complex field is unitary if and only if its inverse matrix coincides with its conjugate transpose:

$U_F^{-1} = U_F$." Ulyanov col. 13, line 65 - col. 14, line 5.

This is different from embedding a constant, such as a trailing 1, into an input data string or program. Furthermore, Ulyanov is silent as to detection of tampering or incorrect execution. Ulyanov therefore cannot and does not teach amended claim 14. We therefore respectfully request withdrawal of the Examiner's rejection.

Dependent Claim 16:

Amended claim 16 depends from claim 15, thus benefiting from like arguments. See the arguments presented in support of claims 1 and 15, above.

Furthermore, Ulyanov does not teach a control computer that embeds one or more constants into a unitary matrix or data string, wherein the results from the host computer indicate tampering or incorrect execution of the encrypted program. The Examiner's cited passage does not teach such limitations, but rather describes standard encoding of a function. Ulyanov nowhere recites or even suggests any means for detection of tampering or incorrect execution of an encrypted program. Withdrawal of the Examiner's rejection of claim 16 is thus respectfully requested.

CONCLUSION

In view of the above clarifying Amendments and Remarks, Applicant respectfully solicits a Notice of Allowance for all of pending claims 1-16.

This Response is filed within the time period for receiving a responsive Advisory Action. However, should any issues remain outstanding, we encourage the Examiner to telephone the undersigned attorney prior to issuing such Advisory Action.

No fees are believed due; however, if any fee is deemed necessary in connection with this Response, please charge Deposit Account No. 12–0600.

Respectfully submitted,

LATHROP & GAGE L.C.

Date: 14 JUL 2006

By: _____

Curtis A. Vock, Reg. No. 38,356
Lathrop & Gage L.C.
4845 Pearl East Circle
Suite 300
Boulder, CO 80301
Tele: (720) 931-3011
Fax: (720) 931-3001